



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/807,990	03/23/2004	Mark Maggenti	000211D13	4659

23696 7590 04/06/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER

TRAORE, FATOUMATA

ART UNIT	PAPER NUMBER
----------	--------------

2109

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/06/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/06/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kscanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/807,990	MAGGENTI ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>03/04</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response of the original filing of March 23, 2004. Claims 1-32 are pending and have been considered below.

Examiner Note

The applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in claims 7, 30 using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer programs modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-3, 13- 16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims do not appear to recite a physical transformation and thus appear not to produce a tangible result. The steps of encrypting, encapsulating, and determining is nothing more than a thought or computation within a processor, both of which are abstract and not a real world result.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1, 4, 7, 13-24, 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6101543) in view of Kluttz et al (US 6598161).

Claims 1, 4, and 7: Alden et al discloses a method, system, and apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

- i. Encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code (the transmit path includes an encryption engine for encrypting the data packet) (column 3, lines 18-19), but does explicitly disclose that a sequential encryption is used.
- ii. Encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);

iii. Encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code the transmit path includes an encryption engine for encrypting the data packet) (column 3, lines 18-19), but does not explicitly disclose that a sequential encryption is used.

iv. Encapsulating said second encrypted data frame in a second transport frame, said second transport frame comprising a first portion and a second portion of said second sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);

v. And transmitting said first transport frame and said second transport frame to a second communication device, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However **Kluttz et al** discloses a secure encryption system, which

used a sequential encryption (the document is then encrypted utilizing at least two encryption keys so as to encrypt the first portion of a document with a first of the at least two encryptions keys and so to encrypt the second portion of the document with a second of the at least two encryption keys) (column 2, lines 9-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Alden et al to use an encryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claims 13, 17, 21: Alden et al discloses a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

- i. Receiving a first transport frame, said first transport frame comprising a first encrypted data payload, a first portion of a first sequential code, and a second portion of said first sequential code (the new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);
- ii. Receiving a second transport frame, said second transport frame comprising a second encrypted data payload, a first portion of a second sequential code, and a second portion of said second sequential code (the

new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);

iii. And determining said second sequential code using said first portion of said second sequential code, said second portion of said second sequential code, and said second portion of said first sequential code, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However **Kluttz et al** discloses a secure encryption system, which used a sequential encryption (the document is then encrypted utilizing at least two encryption keys so as to encrypt the first portion of a document with a first of the at least two encryptions keys and so to encrypt the second portion of the document with a second of the at least two encryption keys) (column 2, lines 9-15). Therefore, it would have been obvious for one having ordinary skills in the

art at the time the invention was made for Alden et al to use an encryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claims 14, 18, 22: Alden et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 13, 17, and 21 above, and Kluttz et al further discloses that decrypting of said second encrypted data payload using said second sequential code (the second portion of the document is decrypted utilizing the second encryption key) (column 2, lines 51-52). Therefore, it would have been obvious for one having ordinary s'kills in the art at the time the invention was made for Alden et al to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claims 15, 19, 23: Alden et al and Kluttz et al disclose a method, system, and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 13, 17, and 21 above, and Kluttz et al further discloses that determining said first sequential code using said first portion of said first sequential code, said second portion of said first sequential code, and said second portion of said second sequential code (the object of the present invention is provided by methods, systems, and computer programs products which encrypt a document by dividing the document into at least a first portion

having a first security and a second portion having a second security level. The document is then encrypted using at least two encryption keys) (column 2, lines 5-11). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Alden et al to distinguish between different portions of the encryption code. One would have been motivate to do so in order to increase data integrity.

Claims 16, 20, 24: Alden et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 15, 19, and 23 above, and Kluttz et al further discloses that decrypting of said first encrypted data payload using said first sequential code (the first portion of the document is decrypted utilizing the first encryption key) (column 2, lines 50-52). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Alden et al to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claims 29, 30, 31, 32: Alden et al discloses a method, system, and apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

Receiving a data frame that is encrypted based on a unique code (the new network adapter further include an interface into a transport layer of the

Art Unit: 2109

local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);

Receiving successive portions of the unique code (the new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);

Alden et al does not disclose that the encryption is based on sequential code encryption. However **Kluttz et al** discloses a secure encryption system, which Determining the unique code (the document is sequentially encrypted utilizing at least two encryptions keys) (column 2, lines 15-16), and further teaches the used of sequential encryption (the document is then encrypted utilizing at least two encryption keys so as to encrypt the first portion of a document with a first of the at least two encryptions keys and so to encrypt the second portion of the document with a second of the at least two encryption keys) (column 2, lines 9-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for **Alden et al** to use an encryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Art Unit: 2109

3. Claims 2, 5, 8, 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6101543) in view of Kluttz et al (US 6598161) in further view of Perlman (US 6363480).

Claims 2, 5, 8, 11: Alden et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 1, 4, 7, and 10 above, but do not explicitly disclose that said first portion of said first sequential code and said first portion of said second sequential code each represent a short-term component of said first and second sequential codes. However, Perlman discloses a system and method for a user to encrypt data in a way that ensures data cannot be decrypted after a finite period, which further short-term component of said first and second sequential codes (provide one or more ephemeral encryption keys to party wishing to encrypt a message to be passed to a destination party (column 2, lines 45-53). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Alden et al to use ephemeral keys in the encryption process. One would have been motivate to do so in order to assure the integrity of the keys.

4. Claims 3, 6, 9, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6101543) in view of Kluttz et al (US 6598161) in further view of Semper (US 6657984).

Art Unit: 2109

Claims 3, 6, 9, 12: Alden et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 1, 4, 7, and 10 above, but do not explicitly disclose the transport frame comprises a radio link protocol (RLP) frame.

However, Semper discloses a system, method, and apparatus for providing backward compatibility of radio link protocols in a wireless network, which further discloses a transport frame, comprises a radio link protocol (the system comprises a radio link protocol) (column 2, lines 10-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Alden et al to use a radio link protocol. One would have been motivate to do so in order to reduce packets loss rate during transmission.

5. Claims 10, 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marino et al (US 6026165) in view of Alden et al (US 6101543) and Kluttz et al (US 6598161).

Claim 10: Marino et al disclose a secure communication comprising:

A receiver (the wireless communication system comprise a receiver)(column 3, lines 26-27);

A transmitter (a plurality of transmitting device) (column 3, lines 27-28);

And a processor communicatively coupled to the receiver and the transmitter, the processor being capable of implementing a method for synchronizing encryption and decryption of a data frame in a communication network (transmission of

encrypted data in a secure system wherein the receiver stores locally an encryption utilized by the transmitting device to encrypt the data message and the receiver uses encryption keys to decrypt an encrypted data message and wherein a sequence number generator is used to synchronously track the message sequence at both the transmitter and the receiver) (abstract), but does not explicitly disclose that the method further comprising:

Encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code; Encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code; Encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code the transmit path includes an encryption engine for encrypting the data packet); Encapsulating said second encrypted data frame in a second transport frame, said second transport frame comprising a first portion and a second portion of said second sequential code; And transmitting said first transport frame and said second transport frame to a second communication device, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code. However, **Alden**

et al discloses a method, system, and apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

1. Encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code (the transmit path includes an encryption engine for encrypting the data packet) (column 3, lines 18-19), but does explicitly disclose that a sequential encryption is used.
2. Encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);
3. Encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code the transmit path includes an encryption engine for encrypting the data packet) (column 3, lines 18-19), but does explicitly disclose that a sequential encryption is used.
4. Encapsulating said second encrypted data frame in a second transport frame, said second transport frame comprising a first portion and a second portion of said second sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);

5. And transmitting said first transport frame and said second transport frame to a second communication device, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However Kluttz et al discloses a secure encryption system, which used a sequential encryption (the document is then encrypted utilizing at least two encryption keys so as to encrypt the first portion of a document with a first of the at least two encryptions keys and so to encrypt the second portion of the document with a second of the at least two encryption keys) (column 2, lines 9-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Marino et al to have a processor coupled to the receiver and the transmitter and to use an encryption based on sequential keys. One would have been motivate to do so in order to increase system efficiency and data integrity.

Claim 25: Marino et al disclose a secure communication comprising:

A receiver (the wireless communication system comprise a receiver)(column 3, lines 26-27);

A transmitter (a plurality of transmitting device) (column 3, lines 27-28);

And a processor communicatively coupled to the receiver and the transmitter, the processor being capable of implementing a method for synchronizing encryption and decryption of a data frame in a communication network (transmission of encrypted data in a secure system wherein the receiver stores locally an encryption utilized by the transmitting device to encrypt the data message and the receiver uses encryption keys to decrypt an encrypted data message and wherein a sequence number generator is used to synchronously track the message sequence at both the transmitter and the receiver) (abstract), but does not explicitly disclose that the method further comprising: receiving a first transport frame, said first transport frame comprising a first encrypted data payload, a first portion of a first sequential code, and a second portion of said first sequential code; receiving a second transport frame, said second transport frame comprising a second encrypted data payload, a first portion of a second sequential code, and a second portion of said second sequential code; and determining said second sequential code using said first portion of said second sequential code, said second portion of said second sequential code, and said second portion of said first sequential code, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the

same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code. Alden et al discloses a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

- iv. Receiving a first transport frame, said first transport frame comprising a first encrypted data payload, a first portion of a first sequential code, and a second portion of said first sequential code (the new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing "received data packet) (column 3, lines 40-45);
- v. Receiving a second transport frame, said second transport frame comprising a second encrypted data payload, a first portion of a second sequential code, and a second portion of said second sequential code (the new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);
- vi. And determining said second sequential code using said first portion of said second sequential code, said second portion of said second sequential code, and said second portion of said first sequential

code, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However **Kluttz et al** discloses a secure encryption system, which used a sequential encryption (the document is then encrypted utilizing at least two encryption keys so as to encrypt the first portion of a document with a first of the at least two encryptions keys and so to encrypt the second portion of the document with a second of the at least two encryption keys) (column 2, lines 9-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for **Marino et al** to have a processor coupled to the receiver and the transmitter and to use an encryption based on sequential keys. One would have been motivate to do so in order to increase system efficiency and data integrity.

Claim 26: **Marino et al**, **Alden et al** and **Kluttz et al** disclose a method, system and apparatus for transmitting packet from a local communications protocol stack

to a virtual private network as in claim 25 above, and Kluttz et al further discloses that decrypting of said second encrypted data payload using said second sequential code (the second portion of the document is decrypted utilizing the second encryption key) (column 2, lines 51-52). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Marino et al to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claim 27: Marino et al, Alden et al and Kluttz et al disclose a method, system, and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 25 above, and Kluttz et al further discloses that determining said first sequential code using said first portion of said first sequential code, said second portion of said first sequential code, and said second portion of said second sequential code (the object of the present invention is provided by methods, systems, and computer programs products which encrypt a document by dividing the document into at least a first portion having a first security and a second portion having a second security level. The document is then encrypted using at least two encryption keys) (column 2, lines 5-11). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Marino et al to distinguish between different portions of the encryption code. One would have been motivate to do so in order to increase data integrity.

Art Unit: 2109

Claim 28: Marino et al , Alden et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 27 above, and Kluttz et al further discloses that decrypting of said first encrypted data payload using said first sequential code (the first portion of the document is decrypted utilizing the first encryption key) (column 2, lines 50-52). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Marino et al to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

6. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Marino et al (US 6026165) in view of Alden et al (US 6101543) and Kluttz et al (US 6598161) and in further view of Perlman (US 6363480).

Claim 11: Marino et al, Alden et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 10 above, but do not explicitly disclose that said first portion of said first sequential code and said first portion of said second sequential code each represent a short-term component of said first and second sequential codes. However, Perlman discloses a system and method for a user to encrypt data in a way that ensures data cannot be decrypted after a finite period, which further short-term component of said first and second sequential codes (provide one or more ephemeral encryption keys to party wishing to

encrypt a message to be passed to a destination party (column 2, lines 45-53).

Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Marino et al to use ephemeral keys in the encryption process. One would have been motivate to do so in order to assure the integrity of the keys.

7. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Marino et al (US 6026165) in view of Alden et al (US 6101543) and Kluttz et al (US 6598161) and in further in view of Semper (US 6657984).

Claim 12: Marino et al, Alden et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 10 above, but do not explicitly disclose the transport frame comprises a radio link protocol (RLP) frame. However, Semper discloses a system, method, and apparatus for providing backward compatibility of radio link protocols in a wireless network, which further discloses a transport frame, comprises a radio link protocol (the system comprises a radio link protocol) (column 2, lines 10-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made for Marino et to use a radio link protocol. One would have been motivate to do so in order to reduce packets loss rate during transmission.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

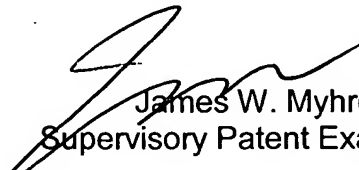
- Scheidt et al (US 6490680) Access control and authorization system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
March 27, 2007


James W. Myhre
Supervisory Patent Examiner